CLAIMS

What is claimed is:

1. A method, comprising:

calculating a first part of a message authentication function by a first processor;

calculating a second part of the message authentication function by a second processor; and

combining the results of the first and second parts into the message authentication code by the first or second processors.

2. The method of claim 1 wherein the message authentication function is used, in part, to authenticate data transmitted between the first processor and a third processor.

3. The method of claim 1 wherein the first and second processors are provided in separate computer systems.

4. The method of claim 1 wherein the first and second parts of the message authentication function consist of one-way hash functions.

5. The method of claim 1 wherein calculating the first part comprises calculating a value without having a data key associated with the function.

6. The method of claim 1 wherein calculating the second part comprises calculating a value for a data set without having contents of the data set.

7. The method of claim 1 further comprising storing the contents into a non-volatile memory coupled to the first processor and storing the message authentication code into non-volatile memory coupled to the second processor.

8. The method of claim 1 further comprising calculating a message authentication code using the message authentication function on a data set,

wherein the message authentication code can be used to authenticate a record that consists of the data set.

9. A method implemented in a first computer, comprising:

creating a record;

computing a first part of a message authentication function using the contents of the record;

providing the result of the first part to a second computer; and

receiving the result of a second part of the message authentication function from the second computer, said second part computed using a data key that is not available to the first computer.

10. The method of claim 9 further comprising encrypting the record and transmitting the record to a third computer.

11. A system, comprising:

a first processor configured to compute a first part of a multi-part message authentication function;

a second processor in communication with the first processor, the second processor is configured to compute a second part of the message authentication function;

wherein the first part of the message authentication function takes the contents of a record and the second part takes a data key, and the first processor does not have the data key and the second processor does not have the record contents.

12. The system of claim 11 wherein the message authentication function is used to authenticate data transmitted between the first processor and a third processor.

13. The system of claim 11 wherein the second processor is configured to compute the message authentication function based on the result of the first

part of the message authentication function computed by the first processor, and the second processor provides the message authentication function result to the first processor to permit the first processor to authenticate the record with the message authentication function and provide the encoded record to a third processor.

14. The system of claim 11 wherein the first processor receives the second part from the second processor and encodes a record with the second part and transmits the encoded record to a third processor.

15. The system of claim 11 wherein the first processor receives the record from a third processor, computes the first part of the message authentication function using the contents of the record, and sends the result of the first part of the message authentication function and the message authentication code in the record to the second processor.

16. The system of claim 11 wherein the second processor is configured to compute the message authentication function based on the result of the first part of the message authentication function computed by the first processor, and the second processor validates the message authentication code provided by, in part, the first processor and received from a third processor in the record, using the message authentication function result.

17. A computer, comprising:

a processor; and

memory containing code executable by said processor;

wherein said executable code causes said processor to compute a first part of a message authentication function including contents of a record, providing the result of said first part to a second computer, receiving the result of a second part of the message authentication function from the second computer, and encoding the record with the result of the second part; and

wherein the record contents are not revealed to the second computer and the second part is computed by the second computer using a data key that is not revealed to the first computer.

18. A method implemented in a first computer, comprising:

receiving a record from a third computer;

computing a first part of a message authentication function using the contents of the record;

providing the result of the first part and the message authentication code in the record to a second computer; and

the second computer computing a second part of the message authentication function based on the result of the first part, using a data key that is not available to the first computer, and validating the message authentication code with the result of the message authentication function.